LESTE

MANUAL DE REGRAS, PROCEDIMENTOS E CONTROLES INTERNOS
(“Manual”)

JULHO/2026

LESTE

ÍNDICE

1. Regras, Procedimentos e Controles Internos

1.1. Apresentação do Grupo Leste

O presente Manual é aplicável à Leste Financial Services Gestão de Recursos Ltda. ("LFS"), Leste Credit Gestão de Recursos Ltda. ("LCBR"), e Leste Administração de Recursos Ltda. ("LAR", e em conjunto com a LFS e LCBR, "Gestoras").

1.2. Objetivo e Aplicabilidade

Este Manual identifica regras, políticas, procedimentos e condutas aplicáveis exclusivamente às Gestoras, considerando a legislação e regulamentação brasileiras.

O presente Manual busca estabelecer normas, princípios, conceitos e valores que orientam a conduta de todos aqueles que possuam cargo, função, posição, relação societária, empregatícia, comercial, profissional, contratual ou de confiança ("Colaboradores") com as Gestoras, tanto na sua atuação interna quanto na comunicação com os diversos públicos, visando ao atendimento de padrões éticos cada vez mais elevados.

Este Manual é parte integrante das regras que regem a relação societária e/ou de trabalho dos Colaboradores, que, ao ingressarem em qualquer uma das Gestoras, receberão cópia do presente Manual. A ausência de manifestação do Colaborador com relação ao teor do Manual será considerada pelas Gestoras como aceitação tácita, assumindo o Colaborador, a partir deste momento, o compromisso constante de observar as normas, princípios, conceitos e valores aqui estabelecidos. Periodicamente, em caso de atualização deste Manual e/ou de outras políticas internas das Gestoras, novas versões poderão ser apresentadas.

As Gestoras e seus Colaboradores não admitem e repudiam qualquer manifestação de preconceitos relacionados à origem, etnia, religião, classe social, sexo, deficiência física ou qualquer outra forma de preconceito que possa existir.

1.3. Base Legal

Todos os Colaboradores devem se assegurar do perfeito entendimento das leis e normas aplicáveis às Gestoras bem como do completo conteúdo deste Manual. São as principais normas aplicáveis às atividades das Gestoras:

(i) Resolução da Comissão de Valores Mobiliários ("CVM") nº 21, de 25 de fevereiro de 2021, conforme alterada ("Resolução CVM 21");

(ii) Resolução CVM nº 50, de 31 de agosto de 2021, conforme alterada ("Resolução CVM 50");
(iii) Resolução CVM nº 175, de 23 de dezembro de 2022, conforme alterada ("Resolução CVM 175") e seus Anexos Normativos;
(iv) Código de Ética da Associação Brasileira das Entidades dos Mercados Financeiro e de Capitais ("ANBIMA" e "Código de Ética");
(v) Código de Administração e Gestão de Recursos de Terceiros ("Código de AGRT");
(vi) Regras e Procedimentos do Código de Administração e Gestão de Recursos de Terceiros, especialmente seu Anexo Complementar III;
(vii) Lei nº 12.846, de 1º de agosto de 2013, e Decreto nº 11.129, de 11 de julho de 2022, conforme alterados ("Normas de Anticorrupção");
(viii) Lei 9.613, de 03 de março de 1998, conforme alterada; e
(ix) Demais manifestações e ofícios orientadores dos órgãos reguladores e autorregulados aplicáveis às atividades das Gestoras.

1.4. Interpretação e Aplicação do Manual

Para fins de interpretação dos dispositivos previstos neste Manual, exceto se expressamente disposto de forma contrária: (a) os termos utilizados neste Manual terão o significado atribuído na Base Legal acima; (b) as referências a Fundos abrangem as Classes e Subclasses, se houver; e (c) as referências a regulamento abrangem os anexos e apêndices, quando aplicável, observado o disposto na Base Legal acima.

1.5. Vigência e Atualização

Este Manual foi elaborado pela Diretoria de *Compliance*, com auxílio do Comitê de *Compliance* e aprovado pelo Comitê Executivo do Grupo Leste.

O presente Manual será revisado, a qualquer tempo, em razão de circunstâncias que demandem tal providência.

1.6. Responsabilidades e Obrigações

A coordenação direta das atividades relacionadas a este Manual é uma atribuição da diretora estatutária indicada como diretora responsável pelo cumprimento de regras, políticas, procedimentos e controles internos das Gestoras ("Diretora de *Compliance*"), nos termos da Resolução CVM 21.

A governança de *compliance* das Gestoras conta com (i) a Diretoria de *Compliance*, formada precipuamente pela Diretora de *Compliance* e por outros Colaboradores que atuem com ela nas atividades abaixo relacionadas ("Equipe de *Compliance*"); e (ii) o Comitê de *Compliance* ("Comitê de Compliance"), formado pela Diretora de *Compliance* (que pode ser assistida por um membro da Diretoria de *Compliance*) e por um

colaborador eleito pelos sócios de cada Gestora, sendo sempre permitido o convite a outros Colaboradores ou consultores externos especializados em *Compliance* como ouvintes.

São obrigações da Equipe de *Compliance* sob a responsabilidade da Diretora de *Compliance*:

(i) Acompanhar as regras descritas neste Manual;
(ii) Levar quaisquer pedidos de autorização, orientação ou esclarecimento ou casos de ocorrência, suspeita ou indício de prática que não esteja de acordo com as disposições deste Manual e das demais normas aplicáveis à atividade das Gestoras para apreciação dos administradores das Gestoras;
(iii) Atender prontamente todos os Colaboradores;
(iv) Identificar possíveis condutas contrárias a este Manual;
(v) Centralizar informações e revisões periódicas dos processos de *compliance*, principalmente quando são realizadas alterações nas políticas vigentes ou se o volume de novos Colaboradores assim exigir;
(vi) Assessorar o gerenciamento dos negócios no que se refere ao entendimento, interpretação e impacto da legislação, monitorando as melhores práticas em sua execução, bem como analisar, periodicamente, as normas emitidas pelos órgãos competentes, como a CVM e outros organismos congêneres;
(vii) Encaminhar aos órgãos de administração das Gestoras, até o **último dia útil do mês de abril** de cada ano, Relatório Anual de *Compliance* ("Relatório Anual de Compliance") referente ao ano civil imediatamente anterior à data de entrega, contendo: ***(a)*** as conclusões dos exames efetuados; ***(b)*** as recomendações a respeito de eventuais deficiências, com o estabelecimento de cronogramas de saneamento, quando for o caso; e ***(c)*** a manifestação do diretor responsável pela administração de carteiras de valores mobiliários de cada uma das Gestoras (indistintamente denominados "Diretor de Gestão") ou, quando for o caso, pelo diretor responsável pela gestão de risco a respeito das deficiências encontradas em verificações anteriores e das medidas planejadas, de acordo com cronograma específico, ou efetivamente adotadas para saná-las; devendo referido relatório permanecer disponível à CVM nas sedes das Gestoras;
(viii) Elaborar relatório **anual** listando as operações identificadas como suspeitas que tenham sido comunicadas às autoridades competentes, no âmbito da Política de Prevenção à Lavagem de Dinheiro, ao Financiamento do Terrorismo e ao Financiamento da Proliferação de Armas de Destruição em Massa – PLDFTP e de Cadastro das Gestoras ("Política de PLDFTP"), devendo referido relatório permanecer disponível à CVM na sede das Gestoras, sendo certo que este relatório de **PLDFTP** poderá constar no mesmo documento do relatório de ***compliance***, mencionado acima;
(ix) Definir os princípios éticos a serem observados por todos os Colaboradores, constantes deste Manual e das outras Políticas internas das Gestoras;
(x) Apreciar todos os casos que cheguem ao seu conhecimento sobre o potencial descumprimento dos preceitos éticos e de *compliance* previstos neste Manual

ou nos demais documentos aqui mencionados, e apreciar e analisar situações não previstas;

(xi) Garantir o sigilo de eventuais denunciantes de delitos ou infrações, mesmo quando estes não solicitarem, exceto nos casos de necessidade de testemunho judicial;

(xii) Solicitar sempre que necessário, para a análise de suas questões, o apoio da auditoria interna ou externa ou outros assessores profissionais;

(xiii) Aplicar as eventuais sanções aos Colaboradores, conforme definido pela Diretoria de *Compliance* ou pelo Comitê de *Compliance*;

(xiv) Analisar situações que cheguem ao seu conhecimento e que possam ser caracterizadas como "conflitos de interesse" pessoais e profissionais. Esses conflitos podem acontecer, inclusive, mas não limitadamente, em situações que envolvam:

- Investimentos pessoais;
- Transações financeiras com clientes fora do âmbito das Gestoras;
- Recebimento de favores/presentes de administradores e/ou sócios de companhias investidas, fornecedores ou clientes;
- Análise financeira ou operação com empresas cujos sócios, administradores ou funcionários, ou Colaborador possua alguma relação pessoal;
- Análise financeira ou operação com empresas em que o Colaborador possua investimento próprio; ou
- Participações em alguma atividade política.

(xv) Promover a ampla divulgação e aplicação dos preceitos éticos no desenvolvimento das atividades de todos os Colaboradores. Nesse sentido, deverá ser realizado um treinamento **inicial**, bem como de reciclagem **anual** de todos os seus Colaboradores, com o objetivo de fazer com que eles estejam sempre atualizados, estando todos obrigados a participar de tais programas de reciclagem. Os treinamentos devem abordar:

- As atividades das Gestoras;
- Os princípios éticos e de conduta das Gestoras;
- As normas de *compliance* das Gestoras;
- As Políticas de Segregação, quando for o caso;
- As demais Políticas descritas neste Manual, especialmente, aquelas relativas à Confidencialidade, Segurança das Informações e Segurança Cibernética, bem como aquelas descritas no Código de Ética, na Política de Investimentos Pessoais e na Política de PLDFTP;
- As penalidades aplicáveis aos Colaboradores decorrentes do descumprimento das regras das Gestoras;

(x) As principais leis e normas aplicáveis às referidas atividades prestadas pelas Gestoras, constantes do item 1.3 deste Manual;

(xi) Assuntos de Certificação, tratados na Política de Certificação, incluindo, sem limitação: (i) as certificações aplicáveis às atividades das Gestoras, suas principais características e os profissionais elegíveis; (ii) explicação de que os Colaboradores que tenham alçada/poder discricionário de decisão de investimento em fundos de investimento financeiros, carteiras administradas e/ou fundos de índice sob gestão

das Gestoras devem, obrigatoriamente, ser isentos ou aprovados na Certificação de Gestores ANBIMA ("CGA") e aqueles que tenham alçada/poder discricionário de decisão de investimento em fundo de investimento em participações, fundos imobiliários, fundos de investimento em direitos creditórios e/ou fundos de índice sob gestão das Gestoras devem, obrigatoriamente, ser isentos ou aprovados na Certificação de Gestores ANBIMA para Fundos Estruturados ("CGE"), devendo os demais buscar a aprovação da decisão de investimento junto ao Diretor de Gestão; e (iii) indicação sobre a necessidade de monitoramento e atualização do Banco de Dados da ANBIMA pela Equipe de *Compliance*.

Ademais, as Gestoras possuirão também Comitê de *Compliance*.

1.7. Garantia de Independência

Os Colaboradores da Equipe de Compliance atuam sob a coordenação da Diretora de *Compliance* e todos exercem suas atividades de forma completamente independente das outras áreas das Gestoras.

1.8. Dúvidas ou ações contrárias aos princípios e normas do Manual

Este Manual possibilita avaliar muitas situações de problemas éticos que podem eventualmente ocorrer no cotidiano das Gestoras, mas seria impossível detalhar todas as hipóteses. É natural, portanto, que surjam dúvidas ao enfrentar uma situação concreta que contrarie as normas de compliance e princípios que orientam as ações das Gestoras.

Em caso de dúvidas ou necessidade de aconselhamento, o Colaborador deve buscar auxílio junto à Diretora de *Compliance*. O e-mail para consultas e informações é compliance@leste.com. Este Manual estará disponível, ainda, no seguinte endereço eletrônico: www.leste.com.

Toda e qualquer solicitação que dependa de autorização, orientação ou esclarecimento expresso da Diretora de *Compliance*, bem como eventual ocorrência, suspeita ou indício de prática por qualquer Colaborador que não esteja de acordo com as disposições deste Manual e das demais normas aplicáveis às atividades das Gestoras, deve ser dirigida à Diretora de *Compliance*.

O Colaborador que tiver conhecimento ou suspeita de ato não compatível com os dispositivos deste Manual deverá reportar, imediatamente, tal acontecimento à Diretora de *Compliance*. Nenhum Colaborador sofrerá retaliação por comunicar, de boa-fé, violações ou potenciais violações a este Manual. O Colaborador que se omitir de tal obrigação poderá sofrer as sanções definidas no item 1.10 deste Manual.

Caso a violação ou suspeita de violação recaia sobre a própria Diretora de *Compliance*, o Colaborador deverá informar diretamente aos demais administradores das Gestoras.

1.9. Acompanhamento das Políticas descritas neste Manual

Mediante ocorrência de descumprimento, suspeita ou indício de descumprimento de quaisquer das regras estabelecidas neste Manual ou aplicáveis às atividades das Gestoras, que cheguem ao conhecimento da Diretora de *Compliance*, de acordo com os procedimentos estabelecidos neste Manual, esta utilizará os registros e sistemas de monitoramento eletrônico referidos neste Manual para verificar a conduta dos Colaboradores envolvidos.

A Equipe de *Compliance*:

(i) Dispõe de sistema interno de arquivo e monitoramento de todos os meios de comunicação utilizados por seus Colaboradores: mensagens de correio eletrônico (e-mail), Teams e *WhatsApp* Business. O referido sistema monitora palavras-chave e reporta à Equipe de Compliance.
(ii) Adicionalmente ao monitoramento descrito acima, a Equipe poderá acessar, quando julgar oportuno e necessário, todo conteúdo que está na rede das Gestoras, inclusive arquivos pessoais salvos em cada computador. Da mesma forma, mensagens de correio eletrônico ou contatos telefônicos de Colaboradores poderão ser gravados e, quando necessário, interceptados e analisados, sem que isto represente invasão da privacidade dos Colaboradores, já que são ferramentas de trabalho disponibilizadas pelas Gestoras;
(iii) Verificará, anualmente, os níveis de controles internos e *compliance* junto a todas as áreas das Gestoras para criação do Relatório Anual de Compliance, com o objetivo de promover ações para esclarecer e regularizar eventuais desconformidades; e
(iv) Analisará os controles previstos neste Manual, bem como em outras políticas das Gestoras, propondo a criação de novos controles e melhorias naqueles que eventualmente sejam considerados deficientes, monitorando as respectivas correções, sendo que as análises e eventuais correções, se for o caso, deverão ser objeto do Relatório Anual de Compliance.

A Diretora de *Compliance* poderá utilizar as informações obtidas nos monitoramentos descritos acima para decidir sobre eventuais sanções a serem aplicadas aos Colaboradores envolvidos, nos termos deste Manual. No entanto, a confidencialidade dessas informações é respeitada e seu conteúdo será disponibilizado ou divulgado somente nos termos e para os devidos fins legais ou em atendimento a determinações judiciais.

1.10. Sanções ("*Enforcement*")

Responsável pela Definição: Diretora de Compliance.

Responsável pela Aplicação: Diretora de Compliance.

Processo Administrativo Interno: Caso seja constatada alguma violação, irregularidade praticada pelo Colaborador ou desvio de conduta em desacordo com os padrões estabelecidos, o Colaborador será chamado a prestar esclarecimentos para a Diretoria de *Compliance* em até 3 (três) oportunidades, a critério da Diretoria de *Compliance*. Caso a Diretoria de *Compliance* entenda que os esclarecimentos não foram suficientes ou a irregularidade não foi sanada, o ato praticado será levado ao superior imediato do Colaborador que contará com o prazo de até 15 (quinze) dias para sanar a irregularidade.

A instauração de Processo Administrativo Interno ocorrerá quando: (i) a irregularidade praticada pelo Colaborador não tenha sido sanada, nem mesmo após o comunicado ao supervisor direto do Colaborador; (ii) a infração incorrida pelo Colaborador for grave; (iii) possa causar prejuízo ao Grupo Leste; ou (iv) tenha sido cometida por um membro da Diretoria, do Comitê de *Compliance* ou do Comitê Executivo do Grupo Leste. As motivações para a instauração do Processo Administrativo Interno previstas nos itens (ii) e (iii) são consideradas situações excepcionais, isto é, a Diretora de *Compliance* poderá, a seu exclusivo entendimento e discricionariedade, instaurar o Processo Administrativo Interno.

A Diretora de *Compliance* deverá levar o Processo Administrativo Interno para análise junto a um fórum colegiado que deverá ser composto pela própria Diretora de *Compliance*, o CEO do Grupo Leste e 1 (um) administrador (Diretor ou Conselheiro) indicado pelo Presidente ou por 5 (cinco) administradores, sendo um deles necessariamente um Conselheiro, caso envolva o CEO. Na segunda hipótese, a Diretora de *Compliance* indicará o Conselheiro que, por sua vez, indicará os outros 4 (quatro) membros. Em caso de empate nas deliberações desse fórum, a Diretora de *Compliance* exercerá o voto de qualidade. Na hipótese de o caso envolver a Diretora de *Compliance*, o fórum colegiado não contará com a própria Diretora de *Compliance*, de forma que será composto pelo CEO e 2 (dois) administradores indicados por este. O voto de qualidade, se necessário, será do CEO.

A Diretora de *Compliance* poderá, a qualquer momento, consultar o Comitê de *Compliance* acerca da matéria objeto de um Processo Administrativo Interno, pautando suas conclusões com base em tal consulta, inclusive no sentido de arquivamento do Processo Administrativo Interno e não envio ao fórum acima mencionado.

Após a conclusão do Processo Administrativo Interno, ponderada a gravidade da ocorrência, o Colaborador pode ser responsabilizado e sujeitar-se a uma das seguintes ações disciplinares:

(i) reprimenda privada, com a assinatura de um termo de compromisso ("Termo de Compromisso Disciplinar");
(ii) suspensão de até 30 dias; ou
(iii) demissão/exclusão do Colaborador.

Durante a análise do Processo Administrativo Interno, são assegurados ao Colaborador a ampla defesa e o direito ao contraditório.

Canal de Denúncias: As Gestoras adotam um canal próprio para que os Colaboradores possam realizar denúncias. A critério do Colaborador, as denúncias poderão ser anônimas. Desta forma, as Gestoras incentivam que os Colaboradores que estejam diante de alguma prática ou suspeite do exercício de alguma prática que viole normas legais, as diretrizes, quaisquer das Políticas e procedimentos deste Manual, faça a comunicação de denúncia através do canal próprio, disponibilizado no endereço eletrônico www.leste.com.

As denúncias encaminhadas pelo canal de denúncias serão recebidas e tratadas pela Diretoria de *Compliance* e, caso tenha se identificado, o Colaborador poderá ser contatado para auxílio nas investigações e/ou *feedback*. Tendo se identificado ou mantido anonimato, a confidencialidade do Colaborador será garantida, sendo absolutamente vedada qualquer forma de retaliação.

Termo de Compromisso Disciplinar: Quando o Processo Administrativo Interno resultar em reprimenda privada, conforme acima descrito, o Colaborador firmará Termo de Compromisso Disciplinar, por meio do qual o Colaborador reconhecerá a violação praticada e reconhecerá igualmente a necessidade de ajuste às normas, com o devido compromisso com a mudança futura.

A finalidade de tal instrumento é a recuperação funcional do envolvido, havendo um prazo estabelecido para a verificação do ajuste de sua conduta, que não poderá superar 60 (sessenta) dias.

O superior imediato é responsável pelo acompanhamento e zelo das condições necessárias para o cumprimento integral do Termo de Compromisso Disciplinar, devendo reportar o acompanhamento sempre que possível à Diretoria de Compliance.

2. Política de Confidencialidade

2.1. Sigilo e Conduta

Todos os Colaboradores deverão ler atentamente e entender o disposto neste Manual, comprometendo-se a seguir condições de confidencialidade aqui presentes.

Nenhuma Informação Confidencial, conforme abaixo definido, deve, em qualquer hipótese, ser divulgada fora das Gestoras. Fica vedada qualquer divulgação, no âmbito pessoal ou profissional, que não esteja em acordo com as normas legais (especialmente, mas não de forma limitada, aquelas indicadas no item 1.3 deste Manual) e de *compliance* das Gestoras.

São consideradas informações confidenciais, reservadas ou privilegiadas ("Informações Confidenciais"), para os fins deste Manual, independente destas informações estarem contidas em *pen-drives*, e-mails, outros tipos de mídia virtual ou em documentos físicos, ou serem escritas, verbais ou apresentadas de modo tangível ou intangível, qualquer informação sobre as Gestoras, sobre as empresas pertencentes ao seu conglomerado, seus sócios e clientes, aqui também contemplados os próprios fundos sob gestão das Gestoras, incluindo:

(i) *Know-how*, técnicas, cópias, diagramas, modelos, amostras, programas de computador;
(ii) Informações técnicas, financeiras ou relacionadas a estratégias de investimento ou comerciais, incluindo saldos, extratos e posições de clientes e dos fundos geridos pelas Gestoras;
(iii) Operações estruturadas, demais operações e seus respectivos valores, analisadas ou realizadas para os fundos de investimento e carteiras geridas pelas Gestoras;
(iv) Estruturas, planos de ação, relação de clientes, contrapartes comerciais, fornecedores e prestadores de serviços;
(v) Informações estratégicas, mercadológicas ou de qualquer natureza relativas às atividades das Gestoras e a seus sócios e clientes, incluindo alterações societárias (fusões, cisões e incorporações), informações sobre compra e venda de empresas, títulos ou valores mobiliários, inclusive ofertas iniciais de ações (*IPO*), projetos e qualquer outro fato que seja de conhecimento em decorrência do âmbito de atuação das Gestoras e que ainda não foi devidamente levado à público;
(vi) Informações a respeito de resultados financeiros antes da publicação dos balanços, balancetes e/ou demonstrações financeiras dos fundos de investimento;

(vii) Transações realizadas e que ainda não tenham sido divulgadas publicamente; e

(viii) Outras informações obtidas junto a sócios, diretores, funcionários, *trainees*, estagiários ou jovens aprendizes das Gestoras ou, ainda, junto a seus representantes, consultores, assessores, clientes, fornecedores e prestadores de serviços em geral.

As Informações Confidenciais não podem ser divulgadas, em hipótese alguma, a terceiros não colaboradores ou a Colaboradores não autorizados, não só durante a vigência de seu relacionamento profissional com as Gestoras, mas também após o seu término.

Os Colaboradores deverão guardar sigilo sobre quaisquer Informações Confidenciais às quais tenham acesso, até sua divulgação ao mercado, bem como zelar para que subordinados e terceiros de sua confiança também o façam, respondendo pelos danos causados na hipótese de descumprimento.

Sem prejuízo da colaboração das Gestoras com as autoridades fiscalizadoras de suas atividades, a revelação de Informações Confidenciais a autoridades governamentais ou em virtude de decisões judiciais, arbitrais e/ou administrativas deverá ser prévia e tempestivamente informada à Diretora de *Compliance*, para que esta decida sobre a forma mais adequada para tal revelação, após serem exauridas todas as medidas jurídicas apropriadas para evitar a supramencionada revelação.

2.2. Dever de Comunicar

Caso os Colaboradores tenham acesso, por qualquer meio, a Informações Confidenciais, deverão levar tal circunstância ao imediato conhecimento da Diretoria de *Compliance*, indicando:

(i) as Informações Confidenciais;

(ii) a razão pela qual ela é material; e

(iii) como, com quem e por que ela foi obtida.

Tal dever de comunicação também será aplicável nos casos em que as Informações Confidenciais sejam conhecidas de forma acidental, em virtude de comentários casuais ou por negligência ou indiscrição das pessoas obrigadas a guardar segredo. Os Colaboradores que, desta forma, acessarem as Informações Confidenciais, deverão abster-se de fazer qualquer uso delas ou comunicá-las a terceiros, exceto quanto à comunicação à Diretora de *Compliance*.

2.3. *Insider Trading, "Dicas" e Front-running*

Em nenhuma hipótese as Informações Confidenciais poderão ser utilizadas para a prática de atos que configurem: **(a)** *Insider Trading*, ou seja, a compra e venda de títulos ou valores mobiliários com base no uso de Informações Confidenciais, com o objetivo de conseguir benefício próprio ou de terceiros (compreendendo os Colaboradores); **(b)** "Dica", ou seja, a transmissão, a qualquer terceiro, estranho às atividades das Gestoras, de Informações Confidenciais que possam ser usadas com benefício na compra e venda de títulos ou valores mobiliários; e/ou **(c)** *Front-running*, ou seja, a prática que envolve aproveitar Informações Confidenciais para realizar ou concluir uma operação antes de outros.

É expressamente proibido valer-se das práticas aqui descritas para obter, para si ou para outrem, vantagem indevida mediante negociação, em nome próprio ou de terceiros, de títulos e valores mobiliários, sujeitando-se o Colaborador às penalidades descritas neste Manual e na legislação aplicável, incluindo eventual demissão por justa causa.

3. Divulgação de Fatos Relevantes

Em que pese seja responsabilidade do administrador fiduciário do fundo a operacionalização da divulgação de qualquer fato relevante ocorrido ou relacionado ao funcionamento do fundo, da classe ou aos ativos integrantes da carteira, assim que dele tiver conhecimento, é responsabilidade dos demais prestadores de serviços, incluindo as Gestoras, informar imediatamente ao administrador fiduciário sobre os fatos relevantes de que venham a ter conhecimento, para a devida divulgação.

Nesse sentido, são considerados relevantes, nos termos do artigo 64, §1º da Parte Geral da Resolução CVM 175, quaisquer fatos que possam influir de modo ponderável no valor das cotas ou na decisão dos investidores de adquirir, resgatar, alienar ou manter cotas.

A seguinte lista não é exaustiva e apresenta exemplos de fatos potencialmente relevantes:

- alteração no tratamento tributário conferido ao fundo, à classe ou aos cotistas;
- contratação de formador de mercado e o término da prestação desse serviço;
- contratação de agência de classificação de risco, caso não estabelecida no regulamento do fundo ou no anexo da classe;
- mudança na classificação de risco atribuída ao fundo, à classe ou à subclasse de cotas;
- alteração de prestador de serviço essencial;
- fusão, incorporação, cisão ou transformação do fundo ou da classe de cotas;

- alteração do mercado organizado em que seja admitida a negociação de cotas do fundo;
- cancelamento da admissão das cotas do fundo ou da classe à negociação em mercado organizado; e
- emissão de cotas de fundo fechado.

Os fatos relevantes podem, de forma excepcional, deixar de ser divulgados, caso seja entendido pelas Gestoras e pelo administrador fiduciário do fundo que sua revelação põe em risco interesse legítimo dos fundos ou de seus cotistas. Neste caso, tais informações serão tratadas como confidenciais até as Gestoras julgarem oportuno o momento para sua divulgação.

Por outro lado, o administrador fiduciário fica obrigado a divulgar imediatamente fato relevante na hipótese de a informação escapar ao controle ou se ocorrer oscilação atípica na cotação, preço ou quantidade negociada de cotas, em havendo negociação em mercado regulado. As Gestoras deverão notificar o administrador fiduciário caso tenha conhecimento de qualquer situação neste sentido.

As Gestoras deverão disponibilizar os fatos relevantes relativos aos fundos sob sua gestão em seu *website*.

4. Políticas de Segurança da Informação e Segurança Cibernética

As medidas de segurança da informação têm por finalidade minimizar as ameaças aos negócios das Gestoras e às disposições deste Manual, buscando, principal, mas não exclusivamente, a proteção de Informações Confidenciais.

As instalações das Gestoras são protegidas por controles de entrada apropriados para assegurar a segurança dos Colaboradores e proteger o sigilo, a integridade e a disponibilidade da informação.

Todos os equipamentos da rede deverão ter acesso restrito. Os computadores que serão utilizados pelos Colaboradores deverão estar seguros e as sessões abertas deverão ser trancadas quando deixadas sem supervisão do Colaborador responsável por seu computador.

O Manual de IT leva em consideração diversos riscos e possibilidades considerando o porte, perfil de risco, modelo de negócio e complexidade das atividades desenvolvidas pelas Gestoras.

A execução direta das atividades relacionadas ao Manual de IT ficará a cargo da Equipe de Compliance que, em conjunto com a equipe de Tecnologia da Informação, será responsável inclusive por sua revisão, realização de testes e treinamento dos Colaboradores, conforme descrito neste Manual.

4.1. Identificação de Riscos (*risk assessment*)

No âmbito de suas atividades, as Gestoras identificaram os seguintes principais riscos internos e externos que precisam de proteção:

(i) Dados e Informações: Informações Confidenciais, incluindo informações a respeito de investidores, clientes, Colaboradores e das Gestoras, operações e ativos investidos pelas carteiras de valores mobiliários sob sua gestão, e as comunicações internas e externas (por exemplo: correspondências eletrônicas e físicas);
(ii) Sistemas: Informações sobre os sistemas utilizados pelas Gestoras e as tecnologias desenvolvidas internamente e por terceiros, suas ameaças possíveis e sua vulnerabilidade;
(iii) Processos e Controles: Processos e controles internos que sejam parte da rotina das áreas de negócio das Gestoras; e
(iv) Governança da Gestão de Risco: Eficácia da gestão de risco pelas Gestoras quanto às ameaças e planos de ação, de contingência e de continuidade de negócios.

Ademais, no que se refere especificamente à segurança cibernética, as Gestoras identificaram as seguintes principais ameaças, nos termos inclusive do Guia de Cibersegurança da ANBIMA:

(i) *Malware* – softwares desenvolvidos para corromper computadores e redes (tais como: Vírus, Cavalo de Troia, *Spyware* e *Ransomware*);
(ii) Engenharia social – métodos de manipulação para obter informações confidenciais (*Pharming*, *Phishing*, *Vishing*, *Smishing*, e *Acesso Pessoal*);
(iii) Ataques de DDoS (*distributed denial of services*) e *botnets*: ataques visando negar ou atrasar o acesso aos serviços ou sistemas da instituição; e
(iv) Invasões (*advanced persistent threats*): ataques realizados por invasores sofisticados utilizando conhecimentos e ferramentas para detectar e explorar fragilidades específicas em um ambiente tecnológico.

Com base no acima, as Gestoras avaliam e definem o plano estratégico de prevenção e acompanhamento para a mitigação ou eliminação do risco, assim como as eventuais

modificações necessárias e o plano de retomada das atividades normais e restabelecimento da segurança devida.

4.2. Ações de Prevenção e Proteção

Após a identificação dos riscos, as Gestoras adotam as medidas a seguir descritas para proteger Informações Confidenciais e sistemas.

- Regra Geral de Conduta

As Gestoras realizam efetivo controle do acesso a arquivos que contemplem Informações Confidenciais em meio físico, disponibilizando-os somente aos Colaboradores que efetivamente estejam envolvidos no projeto que demanda o seu conhecimento e análise.

É terminantemente proibido que os Colaboradores façam cópias (físicas ou eletrônicas) ou imprimam os arquivos utilizados, gerados ou disponíveis na rede das Gestoras e circulem em ambientes externos às Gestoras com estes arquivos, uma vez que tais arquivos contêm informações que são consideradas confidenciais.

A proibição acima referida não se aplica quando as cópias (físicas ou eletrônicas) ou a impressão dos arquivos forem em prol da execução e do desenvolvimento dos negócios e dos interesses das Gestoras. Nestes casos, o Colaborador que estiver na posse e guarda da cópia ou da impressão do arquivo que contenha Informações Confidenciais será o responsável direto por sua boa conservação, integridade e manutenção de sua confidencialidade.

A troca de informações entre os Colaboradores das Gestoras deve sempre se pautar no conceito de que o receptor deve ser alguém que necessita receber tais informações para o desempenho de suas atividades e que não está sujeito a nenhuma barreira que impeça o recebimento daquela informação. Em caso de dúvida a Equipe de *Compliance* deve ser acionada previamente à revelação.

Neste sentido, os Colaboradores não deverão, em qualquer hipótese, deixar em suas respectivas estações de trabalho ou em outro espaço físico das Gestoras qualquer documento que contenha Informações Confidenciais durante a ausência do respectivo usuário, principalmente após o encerramento do expediente.

Qualquer impressão de documentos deve ser imediatamente retirada da máquina impressora, pois pode conter informações restritas e confidenciais mesmo no ambiente interno das Gestoras.

As Gestoras não mantêm arquivo físico centralizado, sendo cada Colaborador responsável direto pela boa conservação, integridade e segurança de quaisquer Informações Confidenciais que estejam em meio físico sob a sua guarda.

O descarte de Informações Confidenciais em meio digital deve ser feito de forma a impossibilitar sua recuperação. Os documentos físicos que contenham Informações Confidenciais ou de suas cópias deverão ser triturados e descartados imediatamente após seu uso de maneira a evitar sua recuperação ou leitura.

Em consonância com as normas internas acima, os Colaboradores devem se abster de utilizar *pen-drives* ou quaisquer outros meios que não tenham por finalidade a utilização exclusiva para o desempenho de suas atividades nas Gestoras. É proibida a conexão de equipamentos na rede das Gestoras que não estejam previamente autorizados pela área de informática das Gestoras.

O envio ou repasse por e-mail de material que contenha conteúdo discriminatório, preconceituoso, obsceno, pornográfico ou ofensivo é também terminantemente proibido, bem como o envio ou repasse de e-mails com opiniões, comentários ou mensagens que possam difamar a imagem e afetar a reputação das Gestoras.

O recebimento de e-mails muitas vezes não depende do próprio Colaborador, mas espera-se bom senso de todos para, se possível, evitar receber mensagens com as características descritas previamente. Neste caso, o Colaborador deve apagá-las imediatamente, de modo que estas permaneçam o menor tempo possível nos computadores das Gestoras.

A visualização de *sites*, *blogs*, *fotologs*, *webmails*, entre outros, que contenham conteúdo discriminatório, preconceituoso (sobre origem, etnia, religião, classe social, opinião política, idade, sexo ou deficiência física), obsceno, pornográfico ou ofensivo é terminantemente proibida.

AÇÕES DE PREVENÇÃO E PROTEÇÃO DE INFORMAÇÕES CONFIDENCIAIS E SEGURANÇA CIBERNÉTICA
Acesso Escalonado do Sistema
O acesso aos sistemas, diretórios, aplicações, bases de dados, e-mails, ferramentas corporativas e demais ativos tecnológicos das Gestoras é concedido de acordo com a função, senioridade, área de atuação e necessidade operacional de cada Colaborador, observando-se o princípio do menor privilégio.

As Gestoras mantêm diferentes níveis de acesso a pastas e arquivos eletrônicos de acordo com as funções e senioridade dos Colaboradores.
A implantação destes controles é projetada para limitar a vulnerabilidade dos sistemas das Gestoras em caso de violação.

A concessão, alteração ou revogação de acessos apenas é realizada mediante solicitação formal, aprovação da área responsável e validação da área de Tecnologia, com aprovação da Diretora de Compliance.

O acesso com perfil administrativo, privilegiado ou equivalente, incluindo administrador local de estação, administrador de sistemas, administrador de diretórios, administrador de ambientes em nuvem, administrador de banco de dados ou acesso a sistemas críticos, é restrito a usuários previamente autorizados e somente quando houver necessidade operacional justificada.

As contas são protegidas por autenticação multifator, segregação de função, registro de atividades, monitoramento, revisão periódica e mecanismos de aprovação ou concessão temporária de acesso.

Os acessos dos colaboradores aos dados corporativos são limitados a regiões onde a Leste possui presença física dos seus escritórios, e liberados temporariamente para usuários que estiverem em viagem a outras regiões.

A implantação destes controles tem como objetivo reduzir a exposição das Gestoras a acessos indevidos, vazamento de informações, alterações não autorizadas, comprometimento de credenciais e demais riscos relacionados à segurança da informação.

Senha e Login

As credenciais de acesso, incluindo login, senha, tokens, certificados, códigos de autenticação, chaves de acesso e demais mecanismos de identidade digital, são pessoais, intransferíveis e de uso exclusivo do respectivo Colaborador.

O Colaborador mantém suas credenciais sob sigilo absoluto, sendo vedado compartilhá-las, divulgá-las, armazená-las de forma insegura, encaminhá-las por e-mail, mensagem instantânea ou qualquer outro meio, ou permitir que terceiros utilizem suas credenciais para acesso a computadores, e-mails, sistemas, aplicações, redes, arquivos ou quaisquer dados das Gestoras.

As Gestoras adotam autenticação multifator, para acesso a e-mail corporativo, sistemas críticos, ambientes em nuvem, acesso remoto, ferramentas administrativas e aplicações que contenham Informações Confidenciais ou dados sensíveis.

As senhas observam os critérios mínimos de segurança definidos pela área de Tecnologia, incluindo requisitos de tamanho, complexidade, reutilização, bloqueio de senhas comprometidas e demais parâmetros técnicos aplicáveis.

A troca de senha é exigida em caso de suspeita ou confirmação de comprometimento, vazamento, compartilhamento indevido, incidente de segurança, alteração relevante de função ou por determinação da área de Tecnologia ou da Diretora de Compliance, seguindo NIST 800-63B.

O Colaborador poderá ser responsabilizado caso disponibilize, compartilhe ou permita o uso indevido de suas credenciais, ainda que o acesso tenha sido realizado por terceiros.

Uso de Equipamentos e Sistemas

Cada Colaborador é responsável pela guarda, conservação e uso adequado dos equipamentos, sistemas, aplicativos, contas, dispositivos e demais recursos tecnológicos colocados à sua disposição pelas Gestoras.

A utilização dos ativos e sistemas das Gestoras, incluindo computadores, telefones, internet, e-mail, ferramentas de colaboração, sistemas internos, aplicações em nuvem e demais recursos tecnológicos, destina-se prioritariamente a fins profissionais. O uso pessoal eventual poderá ser tolerado, desde que não comprometa a segurança, produtividade, disponibilidade, reputação, conformidade regulatória ou os interesses das Gestoras.

É vedado ao Colaborador instalar softwares não autorizados, remover ou desabilitar controles de segurança, alterar configurações corporativas, conectar dispositivos não autorizados, utilizar contas pessoais para fins profissionais ou transferir Informações Confidenciais para ambientes externos sem autorização adequada.

Os equipamentos corporativos possuem controles de segurança compatíveis com sua finalidade, incluindo criptografia de disco, bloqueio automático de tela, proteção contra malware, EDR, firewall local, atualização de sistema operacional, inventário, gerenciamento centralizado e bloqueio contra dispositivos para armazenamento externo de dados.

Caso algum Colaborador identifique perda, furto, roubo, mau funcionamento, uso indevido, violação, suspeita de comprometimento ou má conservação de qualquer equipamento, sistema ou ativo tecnológico, deverá comunicar imediatamente a área de Tecnologia e a Diretora de Compliance.

Acesso Remoto
As Gestoras permitem o acesso remoto ao e-mail, rede, diretórios, sistemas e aplicações corporativas, desde que observados os controles de segurança definidos pela área de Tecnologia em conjunto com a Diretoria de Compliance. O acesso remoto ocorre, sempre que justificável, por meio de dispositivos autorizados, autenticação multifator, conexão segura, políticas de acesso condicional, monitoramento de sessão e demais mecanismos técnicos considerados adequados pela área de Tecnologia. Os Colaboradores autorizados a trabalhar remotamente seguem as diretrizes: (i) utilizar apenas dispositivos protegidos por senha, biometria ou outro mecanismo de autenticação; (ii) manter atualizados os softwares, sistemas operacionais e ferramentas de proteção exigidos pela área de Tecnologia da Informação; (iii) não armazenar Informações Confidenciais ou sensíveis em dispositivos pessoais, salvo autorização expressa e adoção dos controles de segurança aplicáveis; (iv) evitar o uso de redes públicas ou inseguras para acesso a informações corporativas; (v) não compartilhar sessões, telas, credenciais, arquivos ou informações corporativas com terceiros não autorizados; e (vi) comunicar imediatamente à área de Tecnologia e à Diretora de Compliance qualquer violação, suspeita de acesso indevido, perda de dispositivo, phishing, malware ou outro incidente de segurança ocorrido durante o trabalho remoto.
Controle de Acesso
O acesso de pessoas estranhas às Gestoras a áreas restritas somente será permitido mediante autorização de Colaborador autorizado, registro de entrada, identificação e acompanhamento durante a permanência nas dependências. Visitantes, prestadores de serviço e terceiros não têm acesso desacompanhado a áreas que contenham equipamentos, documentos, estações de trabalho, salas técnicas, arquivos físicos, servidores, dispositivos de rede ou Informações Confidenciais. Os Colaboradores zelam para que documentos confidenciais, telas, impressões, dispositivos removíveis, notebooks, telefones corporativos e demais ativos não fiquem expostos a pessoas não autorizadas. As Gestoras utilizam controles de acesso físico, registros de entrada e saída, câmeras de segurança, crachás, segregação de áreas e demais mecanismos destinados à

proteção de suas instalações, ativos e informações.

Firewall, Software*, Varreduras e *Backup
As Gestoras utilizam soluções de segurança destinadas a prevenir, detectar e responder a acessos não autorizados, conexões indevidas, códigos maliciosos, tentativas de intrusão, vazamento de informações e outros eventos de segurança cibernética. A área de Tecnologia é responsável por definir, implementar e manter controles como firewall, segmentação de rede, proteção de endpoints, EDR, antivírus/antimalware, filtros de e-mail, proteção contra phishing, controle de dispositivos, hardening, atualização de sistemas, gestão de vulnerabilidades e demais ferramentas consideradas adequadas ao ambiente tecnológico das Gestoras. Serão conduzidas varreduras periódicas para identificação de vulnerabilidades, configurações inadequadas, softwares desatualizados, riscos de segurança e eventuais programas maliciosos que possam afetar os ativos tecnológicos das Gestoras. A área de Tecnologia é responsável por avaliar, priorizar e aplicar correções de segurança, patches e atualizações relevantes, considerando a criticidade dos ativos, a severidade das vulnerabilidades e o risco para as Gestoras. As Gestoras deverão manter rotinas de backup consideradas adequadas pela área de Tecnologia da Informação, de acordo com a criticidade dos sistemas, dados e processos de negócio. Os backups deverão ser protegidos contra acesso indevido, perda, alteração não autorizada, exclusão acidental ou exclusão maliciosa. Sempre que tecnicamente viável, deverão ser adotados mecanismos de retenção, criptografia, cópias segregadas, armazenamento seguro e proteção contra ransomware. A periodicidade dos backups é definida pela área de Tecnologia, em conjunto com a Diretoria de Compliance, com base na relevância dos sistemas e informações protegidas. É observada a prática de retenção de backups em camadas, GFS, contemplando retenções diárias, mensais, semestrais, anuais e de longo prazo, inclusive por período de até 5 anos, de acordo com a criticidade dos dados, requisitos legais, regulatórios e operacionais aplicáveis. A área de Tecnologia realiza testes periódicos de restauração, de modo a avaliar a efetividade dos backups e a capacidade de recuperação dos dados e sistemas em caso de falha, indisponibilidade, exclusão indevida, incidente cibernético ou desastre.

4.3. Monitoramento e Testes

As Equipes de Tecnologia e de Compliance adotam medidas para monitorar o cumprimento desta política e avaliar a efetividade dos controles de segurança da informação e segurança cibernética.

As medidas incluem, em periodicidade compatível com o risco e, no mínimo, anual:

(i) revisão de acessos a sistemas, pastas, diretórios, aplicações críticas e ambientes em nuvem;
(ii) verificação de aderência às regras de segregação de função, menor privilégio e restrição de acesso;
(iii) análise de logs, eventos de segurança e alertas relevantes;
(iv) testes de restauração de backup;
(v) varreduras de vulnerabilidade e acompanhamento de correções;
(vi) revisão de contas privilegiadas, acessos administrativos e exceções;
(vii) campanhas de conscientização ou simulações de phishing;
(viii) avaliação de incidentes ocorridos e respectivos planos de ação; e
(ix) revisão dos procedimentos de resposta a incidentes, continuidade e recuperação.

4.4. Plano de Identificação e Resposta

- Identificação de Suspeitas

Qualquer suspeita de infecção, acesso não autorizado, outro comprometimento da rede ou dos dispositivos das Gestoras (incluindo qualquer violação efetiva ou potencial), ou ainda no caso de vazamento de quaisquer Informações Confidenciais, mesmo que de forma involuntária, deverá ser informada à Diretora de *Compliance* prontamente. A Diretora de *Compliance* determinará quais membros da administração das Gestoras e, se aplicável, de agências reguladoras e de segurança pública, deverão ser notificados.

Ademais, a Diretora de *Compliance* determinará quais clientes ou investidores, se houver, deverão ser contatados com relação à eventual violação.

- Procedimentos de Resposta

A Diretora de *Compliance* responderá a qualquer informação de suspeita de infecção, acesso não autorizado ou outro comprometimento da rede ou dos dispositivos das Gestoras de acordo com os critérios abaixo:

(i) Avaliação do tipo de incidente ocorrido (por exemplo, infecção de *malware*, intrusão da rede, furto de identidade), as informações acessadas e a medida da respectiva perda;
(ii) Identificação de quais sistemas, se houver, devem ser desconectados ou de outra forma desabilitados;
(iii) Determinação dos papéis e responsabilidades do pessoal apropriado;
(iv) Avaliação da necessidade de recuperação e/ou restauração de eventuais serviços que tenham sido prejudicados;
(v) Avaliação da necessidade de notificação de todas as partes internas e externas apropriadas (por exemplo, clientes ou investidores afetados, segurança pública);
(vi) Avaliação da necessidade de publicação do fato ao mercado, nos termos da regulamentação vigente, (por exemplo: em sendo Informações Confidenciais de fundo de investimento sob gestão das Gestoras, a fim de garantir a ampla disseminação e tratamento equânime da Informação Confidencial);
(vii) Determinação do responsável (ou seja, as Gestoras ou o cliente ou investidor afetado) que arcará com as perdas decorrentes do incidente. A definição ficará a cargo da Diretora de *Compliance*, após a condução de investigação e uma avaliação completa das circunstâncias do incidente.

4.5. Arquivamento de Informações

Os Colaboradores deverão manter arquivada, pelo prazo regulamentar aplicável, toda e qualquer informação, bem como documentos e extratos que venham a ser necessários para a efetivação satisfatória de possível auditoria ou investigação em torno de possíveis investimentos e/ou clientes suspeitos de corrupção e/ou lavagem de dinheiro, bem como todos os documentos e informações exigidos pela Resolução CVM 21, correspondência, interna e externa, papéis de trabalho, relatórios e pareceres relacionados com o exercício de suas funções em conformidade com o inciso IV do Artigo 18 e com o Artigo 34 da Resolução CVM 21.

5. Propriedade Intelectual

Todos os documentos e arquivos, incluindo, sem limitação, aqueles produzidos, modificados, adaptados ou obtidos pelos Colaboradores, relacionados, direta ou indiretamente, com suas atividades profissionais junto às Gestoras, tais como minutas de contrato, memorandos, cartas, fac-símiles, apresentações a clientes, e-mails, correspondências eletrônicas, arquivos e sistemas computadorizados, planilhas, fórmulas, planos de ação, bem como modelos de avaliação, análise e gestão, em qualquer formato, são e permanecerão sendo propriedade exclusiva das Gestoras, razão pela qual o Colaborador compromete-se a não utilizar tais documentos, no presente ou no futuro, para quaisquer fins que não o desempenho de suas atividades nas Gestoras, devendo todos os documentos permanecer em poder e sob a custódia

das Gestoras, sendo vedado ao Colaborador, inclusive, apropriar-se de quaisquer desses documentos e arquivos após seu desligamento das Gestoras, salvo se autorizado expressamente pelas Gestoras e ressalvado o disposto abaixo.

Caso um Colaborador, ao ser admitido, disponibilize às Gestoras documentos, planilhas, arquivos, fórmulas, modelos de avaliação, análise e gestão ou ferramentas similares para fins de desempenho de sua atividade profissional junto às Gestoras, o Colaborador desde já se compromete, junto às Gestoras, a seguir as regras definidas neste Manual, confirmando que: (i) a utilização ou disponibilização de tais documentos e arquivos não infringe quaisquer contratos, acordos ou compromissos de confidencialidade, bem como não viola quaisquer direitos de propriedade intelectual de terceiros; e (ii) quaisquer alterações, adaptações, atualizações ou modificações, de qualquer forma ou espécie, em tais documentos e arquivos serão de propriedade exclusiva das Gestoras, sendo que o Colaborador não poderá apropriar-se ou fazer uso de tais documentos e arquivos alterados, adaptados, atualizados ou modificados após seu desligamento das Gestoras, exceto se aprovado expressamente pelas Gestoras.

6. *Website* das Gestoras

O *website* das Gestoras deverá disponibilizar as Políticas exigidas pela Resolução CVM 21, bem como poderá disponibilizar documentos e informações relativos aos fundos sob gestão, quando aplicável. [1]

7. Política de Anticorrupção

7.1. Introdução e Abrangência das Normas de Anticorrupção

As Gestoras estão sujeitas às normas e leis de anticorrupção, incluindo, mas não se limitando, às Normas de Anticorrupção, as quais estabelecem que as pessoas jurídicas serão responsabilizadas objetivamente, nos âmbitos administrativo e civil, pelos atos lesivos praticados por seus sócios e colaboradores contra a administração pública, nacional ou estrangeira, sem prejuízo da responsabilidade individual do autor, coautor ou partícipe do ato ilícito, na medida de sua culpabilidade.

Considera-se agente público ("Agente Público") e, portanto, sujeito às Normas de Anticorrupção, sem limitação: (i) qualquer indivíduo que, mesmo que temporariamente e sem compensação, esteja a serviço, empregado ou mantendo uma função pública em

[1] Os documentos poderão ser, alternativamente, disponibilizados exclusivamente no site do administrador fiduciário, conforme alinhamento entre os Prestadores de Serviços Essenciais: demonstração de desempenho, lâmina, regulamentos, anexos e apêndices, descrição da tributação aplicável ao Fundo ou à Classe.

entidade governamental, entidade controlada pelo governo, ou entidade de propriedade do governo; (ii) qualquer indivíduo que seja candidato ou esteja ocupando um cargo público; e (iii) qualquer partido político ou representante de partido político.

Considera-se administração pública estrangeira os órgãos e entidades estatais ou representações diplomáticas de país estrangeiro, de qualquer nível ou esfera de governo, bem como as pessoas jurídicas controladas, direta ou indiretamente, pelo poder público de país estrangeiro e as organizações públicas internacionais.

As mesmas exigências e restrições também se aplicam aos familiares de funcionários públicos até o segundo grau (cônjuges, filhos e enteados, pais, avós, irmãos, tios e sobrinhos).
Representantes de fundos de pensão públicos, cartorários e assessores de funcionários públicos também devem ser considerados Agentes Públicos para os propósitos desta Política de Anticorrupção e das Normas de Anticorrupção.

Qualquer violação desta Política de Anticorrupção e das Normas de Anticorrupção pode resultar em penalidades civis e administrativas severas para as Gestoras e/ou seus Colaboradores, bem como impactos de ordem reputacional, sem prejuízo de eventual responsabilidade criminal dos indivíduos envolvidos.

7.2. Definição

Nos termos das Normas de Anticorrupção, constituem atos lesivos contra a administração pública, nacional ou estrangeira, todos aqueles que atentem contra o patrimônio público nacional ou estrangeiro, contra princípios da administração pública ou contra os compromissos internacionais assumidos pelo Brasil, assim definidos:

(i) Prometer, oferecer ou dar, direta ou indiretamente, vantagem indevida a Agente Público, ou a terceira pessoa a ele relacionada;
(ii) Comprovadamente, financiar, custear, patrocinar ou de qualquer modo subvencionar a prática dos atos ilícitos previstos nas Normas de Anticorrupção;
(iii) Comprovadamente utilizar-se de interposta pessoa física ou jurídica para ocultar ou dissimular seus reais interesses ou a identidade dos beneficiários dos atos praticados;
(iv) No tocante a licitações e contratos:
a. frustrar ou fraudar, mediante ajuste, combinação ou qualquer outro expediente, o caráter competitivo de procedimento licitatório público;
b. impedir, perturbar ou fraudar a realização de qualquer ato de procedimento licitatório público;
c. afastar ou procurar afastar licitante, por meio de fraude ou oferecimento de vantagem de qualquer tipo;
d. fraudar licitação pública ou contrato dela decorrente;

e. criar, de modo fraudulento ou irregular, pessoa jurídica para participar de licitação pública ou celebrar contrato administrativo;
f. obter vantagem ou benefício indevido, de modo fraudulento, de modificações ou prorrogações de contratos celebrados com a administração pública, sem autorização em lei, no ato convocatório da licitação pública ou nos respectivos instrumentos contratuais; ou
g. manipular ou fraudar o equilíbrio econômico-financeiro dos contratos celebrados com a administração pública.
(v) Dificultar atividade de investigação ou fiscalização de órgãos, entidades ou agentes públicos, ou intervir em sua atuação, inclusive no âmbito das agências reguladoras e dos órgãos de fiscalização do sistema financeiro nacional.

7.3. Normas de Conduta

É terminantemente proibido dar ou oferecer qualquer valor ou presente a Agente Público sem autorização prévia da Diretora de *Compliance*.

Os Colaboradores deverão se atentar, ainda, que (i) qualquer valor oferecido a Agentes Públicos, por menor que seja, poderá caracterizar violação às Normas de Anticorrupção e ensejar a aplicação das penalidades previstas; e (ii) a violação às Normas de Anticorrupção estará configurada mesmo que a oferta de suborno seja recusada pelo Agente Público.

Os Colaboradores deverão questionar a legitimidade de quaisquer pagamentos solicitados pelas autoridades ou funcionários públicos que não encontram previsão legal ou regulamentar.

Nenhum sócio ou colaborador poderá ser penalizado devido a atraso ou perda de negócios resultantes de sua recusa em pagar ou oferecer suborno a Agentes Públicos.

7.4. Proibição de Doações Eleitorais

As Gestoras não farão, em hipótese alguma, doação a candidatos e/ou partidos políticos via pessoa jurídica. Em relação às doações individuais dos Colaboradores, estes têm a obrigação de seguir estritamente a legislação vigente.

7.5. Relacionamentos com Agentes Públicos

Quando se fizer necessária a realização de reuniões e audiências (“Audiências”) com Agentes Públicos, sejam elas internas ou externas, as Gestoras serão representadas por, ao menos, 2 (dois) Colaboradores, que deverão se certificar de empregar a cautela exigida para a ocasião, com o objetivo de resguardar as Gestoras contra condutas ilícitas no relacionamento com Agentes Públicos. Dentre os procedimentos adotados,

os Colaboradores que estiverem representando as Gestoras deverão elaborar relatórios de tais Audiências e apresentá-los à Diretora de *Compliance* imediatamente após sua ocorrência.

8. Política de Certificação

8.1. Introdução

As Gestoras observam as disposições das Regras e Procedimentos de Certificação ANBIMA, devendo garantir que todos os profissionais elegíveis estejam devidamente certificados.

8.2. Atividades Elegíveis e Critérios de Identificação.

Tendo em vista a atuação das Gestoras como gestora de recursos de terceiros, foi identificado que a Certificação de Gestores ANBIMA ("CGA") e a Certificação de Gestores ANBIMA para Fundos Estruturados ("CGE") são as certificações pertinentes às suas atividades, aplicáveis aos profissionais com alçada/poder discricionário de investimento.

Nesse sentido, somente o Colaborador com poder final para ordenar a compra ou venda de posições, sem a necessidade de aprovação prévia do Diretor de Gestão, ou seja, o Colaborador que tenha, de fato, alçada/poder discricionário de investimentos, é elegível à CGA e CGE, a depender do investimento gerido, uma vez que a CGA é a certificação aplicável aos profissionais que atuam em carteiras administradas, fundos de investimento financeiros e/ou fundos de índice e a CGE é aplicável aos profissionais que atuam em fundo de investimento em participações, fundo de índice, fundo de investimento em direitos creditórios e/ou fundo de investimento imobiliário.

Em complemento, as Gestoras destacam que as certificações são de cunho pessoal e intransferíveis, bem como seguirão os seguintes prazos, os quais serão monitorados pela Diretora de *Compliance*, sendo certo que caso o Colaborador esteja exercendo a atividade elegível de CGA ou CGE nas Gestoras e a certificação não esteja vencida, a partir do vínculo do Colaborador com as Gestoras, o prazo de validade da certificação CGA e CGE será indeterminado, enquanto perdurar o seu vínculo com as Gestoras e a sua atuação na atividade elegível. Por outro lado, caso o Colaborador não esteja exercendo a atividade elegível da CGA ou CGE nas Gestoras, a validade da respectiva certificação será de 3 (três) anos, contados da data de aprovação no exame, ou da data em que deixou de exercer a atividade elegível da CGA ou CGE, conforme o caso.

8.3. Identificação de Profissionais Certificados e Atualização do Banco de Dados

Antes da contratação, admissão ou transferência de área de qualquer Colaborador, a Equipe de *Compliance* deverá solicitar esclarecimentos ou confirmar junto ao supervisor direto do potencial Colaborador o cargo e as funções a serem desempenhadas, avaliando a necessidade de certificação, bem como verificar no Banco de Dados da ANBIMA se o Colaborador possui alguma certificação ANBIMA, uma vez que, em caso positivo, as Gestoras deverão inserir o Colaborador no Banco de Dados da ANBIMA.

O Diretor de Gestão deverá esclarecer à Equipe de Compliance se Colaboradores que integrarão o departamento técnico envolvido na gestão de recursos terão ou não alçada/poder discricionário de decisão de investimento e com quais produtos cada um dos Colaboradores irá atuar.

Caso seja identificada a necessidade de certificação, a Equipe de *Compliance* deverá solicitar a comprovação da certificação pertinente ou sua isenção, se aplicável, anteriormente ao ingresso do novo Colaborador.

A Equipe de *Compliance* também deverá checar se Colaboradores que estejam se desligando das Gestoras estão indicados no Banco de Dados da ANBIMA como profissionais elegíveis/certificados vinculados à Gestora, sendo, para estes, obrigatória a inclusão do desligamento no Banco de Dados da ANBIMA.

A Equipe de *Compliance* deve incluir no Banco de Dados da ANBIMA as informações cadastrais de todos os Colaboradores que tenham qualquer certificação ANBIMA, esteja a certificação vencida e/ou em processo de atualização, sendo referida inclusão facultativa somente para estagiários e terceiros contratados.

Todas as atualizações no Banco de Dados da ANBIMA devem ocorrer **até o último dia útil do mês subsequente à data do evento que deu causa à atualização**, sendo que a manutenção das informações contidas no Banco de Dados da ANBIMA deverá ser objeto de análise e confirmação pela Equipe de *Compliance*, conforme disposto abaixo.

8.4. Rotinas de Verificação

Na periodicidade exigida pela norma aplicável, a Equipe de *Compliance* deverá verificar as informações contidas no Banco de Dados da ANBIMA, a fim de garantir que todos os profissionais certificados/em processo de certificação, conforme aplicável, estejam devidamente identificados, bem como se as certificações estão dentro dos prazos de validade estabelecidos nas Regras e Procedimentos de Certificação ANBIMA.

Ainda, o Diretor de Gestão deverá contatar a Equipe de *Compliance* **prontamente**, sempre que houver algum tipo de alteração nos cargos/funções dos Colaboradores que integram o departamento técnico envolvido na gestão de recursos e/ou nos produtos com os quais cada um desses Colaboradores atue, confirmando, além disso, todos aqueles Colaboradores que atuem com alçada/poder discricionário de investimento, se for o caso.

Colaboradores que não tenham CGA ou CGE, conforme aplicável (e que não tenham a isenção concedida pelo Conselho de Certificação), estão impedidos de ordenar a compra e venda de ativos sem a aprovação prévia do Diretor de Gestão, tendo em vista que não possuem alçada/poder final de decisão para tanto.

Ademais, no curso das atividades de compliance e fiscalização desempenhadas pela Equipe de *Compliance*, caso seja verificada qualquer irregularidade com as funções exercidas por Colaborador, incluindo, sem limitação, a tomada de decisões de investimento sem autorização prévia do Diretor de Gestão por profissionais não certificados ou, de maneira geral, que o Colaborador está atuando em atividade elegível sem a certificação pertinente ou com a certificação vencida, a Diretora de *Compliance* deverá declarar, de imediato, o afastamento do Colaborador, devendo tal diretora, ainda, apurar potenciais irregularidades e eventual responsabilização dos envolvidos, inclusive dos superiores do Colaborador, conforme aplicável, bem como traçar um plano de adequação.

Sem prejuízo do disposto acima, na periodicidade exigida pela norma aplicável, deverão ser discutidos os procedimentos e rotinas de verificação para cumprimento das Regras e Procedimentos de Certificação ANBIMA, sendo que as análises e eventuais recomendações, se for o caso, deverão ser objeto do Relatório Anual de Compliance.

8.5. Processo de Afastamento

Todos os profissionais não certificados ou em processo de certificação, e para os quais haja certificação exigível, nos termos previstos neste Manual, serão imediatamente afastados das atividades elegíveis aplicáveis, até que se certifiquem ou até que o Conselho de Certificação conceda a isenção de obtenção da certificação aplicável.

ANEXO I
TERMO DE COMPROMISSO DISCIPLINAR

Eu,_____, inscrito(a) no CPF/MF sob o nº _____, na qualidade de colaborador do Grupo Leste, pelo presente instrumento, atesto que:

(i) Recebi uma cópia do Manual de Regras, Procedimentos e Controles Internos, Código de Ética e Condutas Internas, da Política de Prevenção à Lavagem de Dinheiro e Cadastro, bem como do Manual de Proteção de Dados (todos, quando referidos em conjunto, denominados simplesmente "Manual");

(ii) Tomei ciência dos direitos e obrigações a que estou sujeito, inclusive no que se refere à responsabilidade sobre informações privilegiadas;

(iii) Li, sanei todas as minhas dúvidas e entendi integralmente as disposições constantes no Manual, incluindo as possíveis sanções decorrentes de condutas contrárias à regulamentação e as responsabilizações daí advindas;

(iv) Estou ciente de que o uso das informações e dos sistemas de informação do Grupo Leste é monitorado, e que os registros assim obtidos poderão ser utilizados para detecção de violações ao Manual e, conforme o caso, servir como evidência em processos administrativos e/ou legais;

(v) Estou ciente de que a política de investimento pessoal, como um todo, juntamente com o Manual passa a fazer parte dos meus deveres como Colaborador do Grupo, incorporando-se às demais regras internas adotadas pelo Grupo Leste;

(vi) Comprometo-me, ainda, a informar imediatamente à Diretoria de *Compliance* qualquer fato que eu venha a ter conhecimento que possa gerar algum risco;

(vii) A partir desta data, a não observância do Termo de Confidencialidade e/ou deste Termo de Compromisso Disciplinar poderá implicar a caracterização de falta grave, fato que poderá ser passível da aplicação das penalidades cabíveis ou desligamento, conforme minha função à época do fato;

(viii) As regras aqui estabelecidas não invalidam nenhuma disposição societária ou contrato de trabalho, nem de qualquer outra regra estabelecida pelo Grupo Leste, mas apenas servem de complemento e esclarecem como lidar com determinadas situações relacionadas à minha atividade profissional;

(ix) Tenho ciência de que, com exceção de autorização escrita da Diretoria de *Compliance*, é expressamente proibido quaisquer investimentos pessoais feitos por mim, meu cônjuge, companheiro ou dependente financeiro, em desacordo com a Política de Investimentos Pessoais das Gestoras;

(x) Os investimentos relacionados em documento anexo a este termo foram realizados anteriormente ao meu ingresso no Grupo Leste e representam a totalidade dos meus investimentos pessoais;

(xi) Participei do processo de treinamento e recebi o Manual. Tive, portanto, conhecimento dos princípios e das normas aplicáveis às minhas atividades e do Grupo Leste e tive oportunidade de esclarecer dúvidas relacionadas a tais princípios e normas junto à Diretoria de Compliance, de modo que as compreendi e me

comprometo a observá-las no desempenho das minhas atividades, bem como a participar assiduamente do programa de treinamento continuado;

(xii) Tenho ciência de que é terminantemente proibido fazer cópias (físicas ou eletrônicas) ou imprimir os arquivos utilizados, gerados ou disponíveis na rede do Grupo Leste e circular em ambientes externos com estes arquivos (físicos ou eletrônicos) sem a devida observância do Manual, uma vez que tais arquivos contêm informações que são consideradas como informações confidenciais, conforme descrito no Termo de Confidencialidade.

(xiii) Tenho ciência de que o Grupo Leste poderá gravar qualquer ligação telefônica realizada ou recebida por meio das linhas telefônicas disponibilizadas pelo Grupo Leste para minha atividade profissional, especialmente, mas não se limitando, às ligações da equipe de atendimento e da mesa de operação das Gestoras;

(xiv) Tenho ciência de que o Grupo Leste poderá monitorar toda e qualquer troca, interna ou externa, de meus e-mails e outras modalidades de comunicação eletrônica;

(xv) Tenho ciência de que a senha e login para acesso aos dados contidos em todos os computadores, inclusive nos e-mails, são pessoais e intransferíveis, de modo que me comprometo a não os divulgar para outros colaboradores do Grupo e/ou quaisquer terceiros;

(xvi) Estou ciente do meu compromisso em comunicar o Encarregado, termo definido no Manual de Proteção de Dados, qualquer situação que chegue ao meu conhecimento que esteja em desacordo com as regras descritas no Manual de Proteção de Dados.

Cidade:
Data:

Declaro para todos os fins que estou de acordo com os termos acima e ciente das minhas obrigações e responsabilidades como colaborador do Grupo Leste.

Assinatura do Colaborador: